

REMARKS/ARGUMENTS

Claims 1-19 and 25-43 are pending in the application and all are rejected as anticipated under 35 U.S.C. 102(e). The rejection is respectfully traversed and reconsideration is requested. The references asserted do not teach or suggest the claimed invention.

Claim Amendments

Amended independent claims 1 and 25, respectively, propose a method and system of single sign-on user access to multiple web servers that involves authenticating a user by a first web server, the first web server also providing a first type of service session functionality for the user in addition to an authentication functionality and detecting a client request for a second type of service session functionality for the user at the first web server that is not provided by the first web server. Amended claims 1 and 25 further propose that the first web server determines a second web server providing the second type of session functionality for the user and in response thereto creates an encrypted, digitally signed authentication token related to the user that has an expiration time, and transmits the encrypted authentication token to the second web server via the user's web browser. In addition, amended claims 1 and 25 propose authenticating the authentication token by the second web server and providing the second type of service session functionality for the user by the second web server. See, e.g., Application p. 4, line 25-p. 12, line 24.

Support for the foregoing amendment is found throughout the specification and in the claims and as detailed above. Accordingly, no new matter has been added.

Claim Rejections - 35 U.S.C. § 102

Claims 1-19 and 25-43 stand rejected as anticipated by the Sasmazel (U.S. Patent No. 6,263,432) under 35 U.S.C. § 102(e). The rejection is respectfully traversed and reconsideration is requested. The reference asserted does not read on the claimed invention.

On the contrary, instead of authenticating the user at a first web server, the first web server also providing a first type of service session functionality for the user in addition to an authentication functionality, as recited in amended independent claims 1 and 25, Sasmazel requires a dedicated authentication server 350 which provides no type of service session functionality other than authentication functionality. According to Sasmazel, when the user submits a sign-on request to the web server 220 or 240, instead of authenticating the user by the web server that provides the service session functionality, the web server of Sasmazel sends the user's sign-on request to the dedicated authentication server 350, which uses authentication information supplied by the user in the sign-on request to generate an "eticket" 310. See, e.g., Sasmazel, Col 7, line 38-Col 10, line 30 and Figs. 6 and 7. Thus, there is no hint of teaching or suggestion in Sasmazel of authenticating the user by a first web server that also provides a first type of service session functionality for the user in addition to the authentication functionality; as recited in amended independent claims 1 and 25.

Nor is there any teaching or suggestion whatsoever in Sasmazel of detecting a client request for a second type of service session functionality for the user at said first web server that is not provided by the first web server, said first web server determining a second web server providing the second type of session functionality for the user and in response thereto creating an encrypted authentication token related to the user and redirecting a web browser of the user to the second web server and transmitting the encrypted authentication token from the first web server to the second web server via the user's web browser, wherein the authentication token comprises an expiration time and is digitally signed by the first web server, as recited in amended claims 1 and 25. On the contrary, instead of detecting a client request for a second type of service session functionality for the user at the first web server that is not provided by the first web server and determining a second web server providing the second type of session functionality for the user by the first web server and in response thereto creating an encrypted authentication token related to the user and redirecting the user's web browser to the second web server and transmitting the

encrypted authentication token from the first web server to the second web server via the user's web browser, as recited in amended claims 1 and 25, according to Sasmazel, after generating the "eticket" 310, the dedicated authentication server 350 simply sends the "eticket" back to the user's browser 210, where it remains until the user signs on again at the same or another web server to request another function, at which time, the "eticket" is sent from the browser to the particular web server 220 or 240, which in turn sends the "eticket" on to a dedicated authorization server 360. See, e.g., Sasmazel, Col 10, lines 9-24 and Fig. 7.

Moreover, there is no hint of teaching or suggestion in Sasmazel of authenticating the authentication token by the second web server and providing the second type of service session functionality for the user at the second web server, as recited in amended claims 1 and 25. Instead, according to Sasmazel, when the user signs on again at the same or another web server to request another function and the "eticket" is sent to the particular web server, the web server sends the "eticket" to the authorization server 360, which performs the authentication and authorization check, and if validated by the authorization server, the validation is returned to the web server. See, e.g., Sasmazel, Col 10, lines 20-30 and Fig. 7.

Consequently, Sasmazel fails to teach the required combinations of limitations of Applicants' method and system of single sign-on user access to multiple web servers that involve authenticating a user by a first web server, the first web server also providing a first type of service session functionality for the user in addition to an authentication functionality, detecting a client request for a second type of service session functionality for the user at said first web server that is not provided by the first web server, said first web server determining a second web server providing the second type of session functionality for the user and in response thereto creating an encrypted authentication token related to the user and redirecting a web browser of the user to the second web server, transmitting the encrypted authentication token from the first web server to the second web server via the user's web browser, wherein the authentication token comprises an expiration time and is digitally signed

by the first web server, authenticating the authentication token by the second web server; and providing the second type of service session functionality for the user by the second web server, as recited in amended claims 1 and 25.

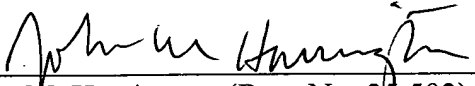
Because each and every element as set forth in amended claims 1 and 25 is not found, either expressly or inherently in the cited reference, the Examiner has failed to establish the required *prima facie* case of unpatentability. See Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628 (Fed. Cir. 1987); See also MPEP §2131. The Examiner has failed to establish the required *prima facie* case of unpatentability for amended independent claims 1 and 25 and similarly has failed to establish a *prima facie* case of unpatentability for claims 2-19 that depend on amended claim 1 and claims 26-43 that depend on amended claim 25, and which recite further specific elements that have no reasonable correspondence with the references.

Conclusion

In view of the foregoing amendment and these remarks, each of the claims remaining in the application is in condition for immediate allowance. Accordingly, the examiner is requested to reconsider and withdraw the rejection and to pass the application to issue. The examiner is respectfully invited to telephone the undersigned at (336) 607-7318 to discuss any questions relating to the application.

Respectfully submitted,

Date: 5/16/05


John M. Harrington (Reg. No. 29,592)
for George T. Marcou (Reg. No. 33,014)

Kilpatrick Stockton LLP
607 14th Street, NW, Suite 900
Washington, DC 20005
(202) 508-5800